

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
30 June 2005 (30.06.2005)

PCT

(10) International Publication Number
WO 2005/060147 A1

(51) International Patent Classification⁷: H04L 9/06

(21) International Application Number:
PCT/IB2004/052607

(22) International Filing Date:
30 November 2004 (30.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03104643.6 11 December 2003 (11.12.2003) EP

(71) Applicant (for all designated States except US): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL];
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): GORISSEN, Paulus, M., H., M., A. [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). TRESCHER, Joachim, A. [DE/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). STARING, Antonius, A., M. [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). MALLON,

Willem, C. [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). TREFFERS, Menno, A. [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

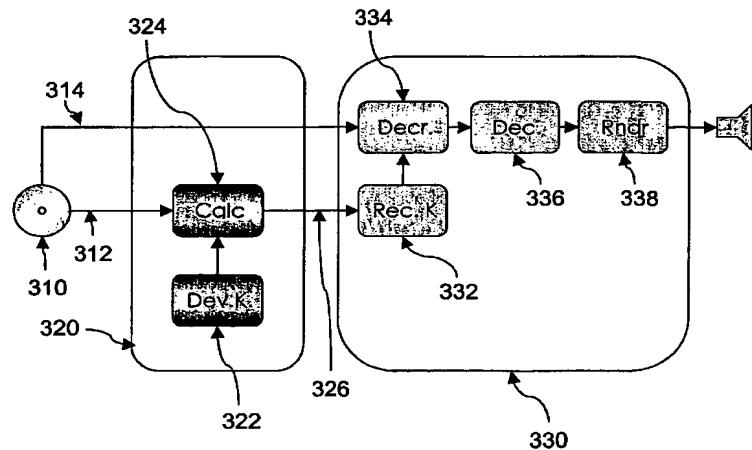
(74) Agents: GROENENDAAL, Antonius, W., M. et al.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE,

[Continued on next page]

(54) Title: BLOCK CIPHERING SYSTEM, USING PERMUTATIONS TO HIDE THE CORE CIPHERING FUNCTION OF EACH ENCRYPTION ROUND



(57) Abstract: In a system (600), a server (610) provides a digital signal processing function f to an executing device (620) in an obfuscated form. The function f includes a function cascade of signal processing functions f_i , $1 \leq i \leq N$ to formula (I). The server includes a processor (612) for selecting a set of $2N$ invertible permutations p_i , $1 \leq i \leq 2N$; calculating a set of N functions g_i , where g_i is functionally equivalent to formula (II) for $1 \leq i \leq N$; and calculating a set of $N-1$ functions h_i , where h_i is functionally equivalent to formula (III) for $2 \leq i \leq N$. The server includes means (614) for equipping the executing device with an execution device function cascade that includes formula (IV), where y_1, \dots, y_N are function parameters to formula (V), and means (616) for providing the functions g_1, \dots, g_N to the executing device. The executing device includes means (626) for obtaining the functions g_1, \dots, g_N and a processor (622) for loading the execution device function cascade and applying the loaded execution device function cascade to the functions g_1, \dots, g_N (e.g., $ED(g_1, \dots, g_N)$).

WO 2005/060147 A1



SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA,*

SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

- *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.